

Involving Older People Project

PERSONAL COMPUTING AND INTERNET SAFETY CONSIDERATIONS

Introduction

This document has been produced to help project participants' gain a balanced understanding of the risks involved in using personal computers on the internet.

While the Internet has transformed and greatly improved our lives, this vast network and its associated technologies have opened the door to an increasing number of security threats from which individuals, families and businesses must protect themselves. This is especially true when we begin to exploit the advantages of online facilities such as e-mail, banking, shopping, discussion groups, and on line auctions.

General points

The threats

As with any type of crime, the threats to your privacy and wellbeing come from a **very small minority**. **Common sense, some simple rules** and a few pieces of **technology** can help protect your computer systems from unauthorised occurrences. All computers, from the family home computer to those on desktops in the largest businesses in the country can be affected by computer security breaches. However, security breaches can often be easily prevented.

Threats and common sense

Just as you would not give a stranger you met in the street details of your bank account etc, the internet is no different do not give your details out to strangers online! A fairly recent example of a scam is that a "Pop up" window appears when you are surfing the net, **do not** click on these as they can take you to sites which are undesirable and/or could cost you money.

The important thing is to "BE SAFE" then you can then enjoy the wonderful world of the Internet.

Involving Older People Project

PERSONAL COMPUTING AND INTERNET SAFETY CONSIDERATIONS

What are the main risks?

- 1) Internet fraud – dishonest people extracting money from your bank accounts or charging unauthorised items to our credit cards.
The extreme version of this activity is identity theft.
- 2) Unwanted attention from people we do not want to know.
- 3) Damage to your computer system's software.

When are we NOT subject to risk?

The lowest level of risk exists when we are using computer while disconnected from the internet.

The project website WWW.ageingmatters.com is safe.

When ARE we at risk?

As soon as we connect to the network some risk exists with respect to computer system software (item 3 above).

Special hardware and software known as firewalls and virus checkers provided with project provided systems address this problem so users need not worry about damage to their system's software.

The use of e-mail introduces risks associated with both fraud and unwanted attention (items 1 and 2).

Item 2 **unwanted attentions** can be reduced to an almost negligible extent by observing the suggestions contained in list 2 (on page 5).

1) Internet Fraud

Resourceful criminals have invented a bewildering and increasingly ingenious variety of "scams" designed to separate us from our money.

As soon as you start to use e-mail, online shopping, online banking or participate in other commercial transactions such as online auctions the risk increases.

That said however observing the guidelines suggested in List 1 (page 3) will help reduce the risk of fraud.

Users of online banking and credit card accounts should be wary of any e-mails requesting information pertaining to their account. For example a request for a password, expiry date or login ID is highly suspect. These requests are sometimes justified on the pretext that the bank (for example) has had a computer failure and needs the information to revalidate your account. **Never respond to such requests.** Contact your bank or credit card company by phone using a number taken from their documentation – **not** any telephone number sent to you in the suspect e-mail. Do not take any links provided in the e-mail as they may direct you to a bogus website to gather information pertinent to your account.

The bank or credit card company's help desk will advise you on what to do next.

Involving Older People Project

PERSONAL COMPUTING AND INTERNET SAFETY CONSIDERATIONS

Suggestion List 1 Fraud Avoidance

Financial transactions

Keep your online banking and credit card company passwords and pin numbers secret from everyone. Change them every 3 months at least.

Enter your bank's website address yourself or from your favourites list do not make use of any link which is sent to you – it could be bogus.

Check you bank/credit card statements carefully. Report anything suspicious to the company involved as soon as possible.

Check you bank and credit card companies' websites for up to date advice on security matters.

Don't be conned by convincing e-mails offering you the chance to make some easy money. If it looks too good to be true it almost certainly is!

Be especially wary of unsolicited e-mails from outside the UK - it will be much harder for you (or the authorities in the event of fraud) to be sure the senders are who they say they are. Generally avoid them.

Online shopping

There are signs to look out for when looking at shopping web sites:

Secure sites have Uniform Resource Locators (URLs) with https:// are their prefix not the normal http://. Additionally a symbol such as an unbroken key or closed padlock on the site certifies that it is secure.

However you should still check the company's terms and conditions some of these security assurances provide only limited cover in the event of loss.

(Please note that in the case of a shopping site such as Argos the https URL only comes into use just before the checkout and payment stage of the buying process).

Here are some of the symbols used to indicate secure shopping sites;



If you decide to shop on the web always read the company's privacy policy to ensure that your address will not be used or passed on in a way which is to your disadvantage.

Online auctions

These are best avoided. If you do decide to trade check on the business record of the buyer or seller you are dealing with and only part with money through an escrow intermediary. An escrow intermediary is a company which holds on to the buyer's money until the buyer has received the goods and is happy to release the money to the seller.

Involving Older People Project
PERSONAL COMPUTING AND INTERNET SAFETY CONSIDERATIONS

Pop Ups

Do not reply "YES" to any pop ups or provide any information on links originating from pop ups. A recent scam (affecting dial up users – not a problem for users on broadband connections) involves redirecting internet dial up connections through expensive alternative routing.

The user ends up with a huge phone bill because he has unwittingly agreed to reroute his connection by clicking "yes" to a pop up.

Involving Older People Project

PERSONAL COMPUTING AND INTERNET SAFETY CONSIDERATIONS

Suggestion List 2 – Avoiding Unwanted Attention

When you begin to use e-mail give some thought to the e-mail address which you chose. Bear in mind that the recipient of an e-mail can only take action based on the information you have provided.

So you might consider using an e-mail address name (e-mail ID) which does not provide any clue to your identity. A name like “Eliza_Doolittle123” might be preferable to “Elizabeth_Dickson”. An unscrupulous person could perhaps combine your name (Elizabeth Dickson) together with a mention in one of your notes of living in the south side of Glasgow to determine your home address. A search of the online electoral role is one way in which this could be done.

E-mail has the facility to insert a closing “signature” in any notes you send. If we include our telephone number and perhaps even our home address in the “signature” we open up another opportunity for unwelcome attention. So if you use this facility give some thought to the signature content.

When you receive an invitation to participate in any kind of deal or discussion group on the internet – it is best not to take up these offers – you have no idea who is behind them. Do not make use of the “opt out” reply option perhaps thinking that this will remove you from a contact list. These replies can be used to identify e-mail addresses which are “active”, the addresses can be sold on attracting even more unsolicited mail.

If you decide to shop on the web always read the company’s privacy policy to ensure that your address will not be used or passed on in a way contrary to your wishes.

Involving Older People Project
PERSONAL COMPUTING AND INTERNET SAFETY CONSIDERATIONS

Suggestion List 3 - Damage to your computer system.

Keep your login password secret and change it periodically.

A firewall and virus checker have been provided on (project) provided systems.
These products are automatically updated regularly.
Security and other updates to Microsoft products will be managed by the project team.

Be careful to whom you allow to access your machine.

Involving Older People Project
PERSONAL COMPUTING AND INTERNET SAFETY CONSIDERATIONS

Assumptions associated with personal computing and internet safety considerations

The following provisos only apply to equipment provided by the project. Care home and personally owned computer equipment used in the project will be used as provided.

The project team responsibility for project provided hardware and software ends on 15 May 2005 when ownership of the project provided systems passes to the user.

Physical;

Personal computers provided by the project will not be provided with cover locks or any media drive locks.

Firewall;

We will install ZoneAlarm with user message suppression.

Virus protection;

AntiVir Personal Edition will be installed.

Fraud;

User guidelines will be provided on a best advice basis.

Ultimately the project cannot be responsible for clients becoming the victim of fraudulent activity.